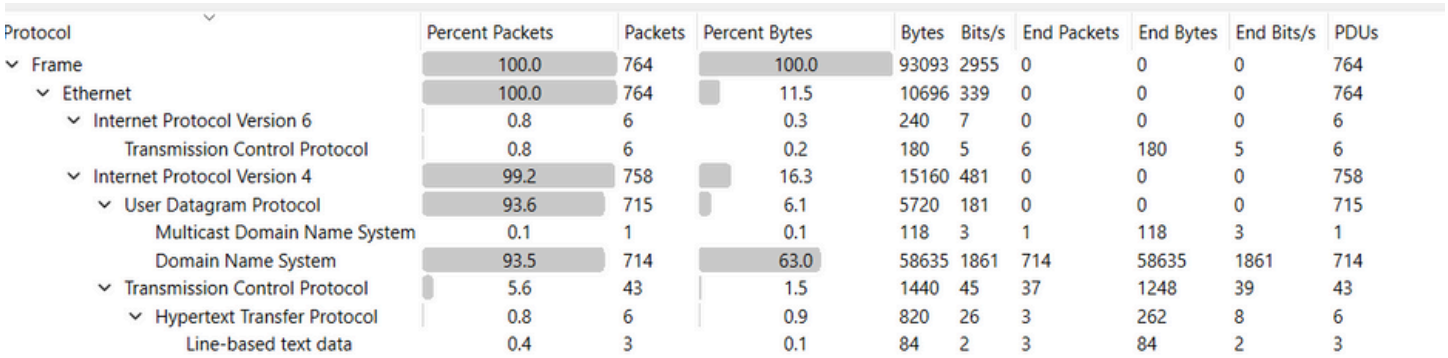
Name - Krish Sharma

Roll No- 110124062

Networking Basic Task - analyzing pcapng file

1. What types of traffic (HTTP, DNS, FTP, etc.) are present?



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	764	100.0	93093	2955	0	0	0	764
Ethernet	100.0	764	11.5	10696	339	0	0	0	764
Internet Protocol Version 6	0.8	6	0.3	240	7	0	0	0	6
Transmission Control Protocol	0.8	6	0.2	180	5	6	180	5	6
Internet Protocol Version 4	99.2	758	16.3	15160	481	0	0	0	758
User Datagram Protocol	93.6	715	6.1	5720	181	0	0	0	715
Multicast Domain Name System	0.1	1	0.1	118	3	1	118	3	1
Domain Name System	93.5	714	63.0	58635	1861	714	58635	1861	714
Transmission Control Protocol	5.6	43	1.5	1440	45	37	1248	39	43
Hypertext Transfer Protocol	0.8	6	0.9	820	26	3	262	8	6
Line-based text data	0.4	3	0.1	84	2	3	84	2	3

there are 6 HTTP packets , 714 DNS ,and no FTP packet present.

(filter used - frame)

2. How many DNS queries were made in total?

filter used - dns.flags.response == 0

358 DNS queries were made

3. What types of DNS queries were made?

A , AAA and HTTPS

4. What is a Loopback Interface?

A loopback interface is a virtual network interface used by a computer to send traffic to itself. i.e. the source is same as the destination.

5. How many .txt files were requested? List their names.

there were 3 txt files requested .

1. decoy1.txt

2. encoded.txt
3. decoy2.txt

6. One .txt file contains base64-encoded content. Identify and decode it. What does it contain?

encoded.txt contains base64-encoded content .

RkxBR3tzcGlkM3JfbmV0d29ya19tYXN0ZXJ9Cg==

decoded - FLAG{spid3r_network_master}

7. Was any attempt made to distract the analyst using decoy files? Explain.

Two .txt files named decoy1.txt and decoy2.txt were present in the traffic.

Typically, decoy files are used to Waste the analyst's time by making them inspect irrelevant files.

8. Are there any known ports being used for uncommon services?

while port 8000 is not "uncommon" in development or local applications, it is not typically used for standard web services in production, making it "uncommon" in general internet traffic compared to ports 80 or 443.

9. How many HTTP GET requests are visible in the capture?

http.request.method == "GET"

there are 3 HTTP GET requests visible

http.request.method == "GET"

	Time	Source	Destination	Protocol	Length	Info
752	242.560779732	127.0.0.1	127.0.0.1	HTTP	153	GET /decoy1.txt HTTP/1.1
180	71.012227833	127.0.0.1	127.0.0.1	HTTP	153	GET /decoy2.txt HTTP/1.1
207	118.183454033	127.0.0.1	127.0.0.1	HTTP	154	GET /encoded.txt HTTP/1.1

10. What User-Agent was used to make the HTTP requests?

user agent is curl/8.5.0\r\n